APPENDIX C
THE COVENANT TRUST MODEL
SELF-CERTIFICATION OF DIGITAL SIGNATURE KEYS BY CONTRACT

Edwin A. Suominen

A. THE COVENANT TRUST MODEL

I. BACKGROUND

With the Electronic Signatures in Global and National Commerce Act of 2000, the U.S. Congress gave digital signatures the same legal validity as an ink signature on a piece of paper. Now, the sender of an email message, word processing document, or any other type of electronic record that can be construed as a written contract can be legally bound to that record if the recipient can prove that the sender authenticated the record.

Electronic records that are signed with digital signatures can be proven, to a very high level of certainty, to be authenticated by the person who caused the digital signature to be applied to the record. The digital signature can only be applied with a private key, which is an incredibly large number that uniquely corresponds to another incredibly large number, called a public key. The private key, as its name implies, is kept a strict secret by the person who uses it to sign his or her digital signature. Strong cryptographic software ensures that it is "computationally infeasible" (i.e., very difficult, even with very fast computers) to derive the private key from the public key. When a person signs an electronic record with their private key, a digital signature code is produced that anyone can verify against the public key, which is publicly accessible. The slightest change in a document so signed will cause the digital signature to no longer match the document.

The cryptography used in digital signatures is very strong and nearly impossible to tamper with, at least with current technology. But a very old problem remains that technology alone cannot entirely solve. That problem is trust.

The trust problem in digital signatures can be summarized as follows: How do you know that the public key really belongs to the person who says it belongs to him or her? Anyone can create a public key and call it someone else's, then use the corresponding private key to create forged electronic records. The 1998 edition of The Global Trust Register, a printed directory of public keys published by a group of cryptography experts, states the problem as follows: "[T]here is no cheap and effective

way for Internet users to check the validity of public keys on which they may wish to rely."

The experts who wrote The Global Trust Register made that statement in spite of the many efforts by Certification Authorities (CAs) to deploy a "hierarchical trust" model, where trusted third parties check out the identity of persons who own private/public key pairs. A CA such as Verisign, Entrust, or Thawte will add its digital signature to a public key if the public key is tied to the name of a person who physically appears with proper documentation to prove their identity. Recipients of documents signed with the certified public key are then expected to trust that the CA has done its job and that the public key really came from the person whose name is tied to it.

But what happens when one of the many employees at the CA doesn't do his or her job properly? Who is liable for the recipient's reliance on a forged document promising delivery of 10,000 widgets for $1M when the sender has pocketed the money and run, completely anonymously due to the faceless nature of the Internet? The recipient cannot sue the sender if the recipient doesn't know the sender really was. The recipient's only course of action is to sue the CA for not doing its job. CAs try to avoid liability with disclaimer language in their Certification Practice Statements.

What about tort claims against the CA? Here's what the text Certification Authority Liability Analysis has to say about that:

> A CA's liability for tort claims based on negligence **may be limited** by the so-called "economic loss doctrine." The economic loss doctrine provides that claims for purely economic losses based on product defects are not recoverable in tort. The rule holds simply that tort liability does not arise for pure economic loss, but only for personal injury or property damage. The principles behind this rule are that protecting personal injury and property damage claims are more important social policies than pure economic (business) losses, and that economic losses are better protected by negotiated contract allocations rather than through generalized tort law. (Certification Authority Liability Analysis Section 1.1, American Banker's Association, 1998, emphasis added.)

In addition to the problems with "hierarchical trust" that should now be apparent, reliance on the Certification Authority as a trusted third party requires the CA to have an established reputation and to keep its digital house in order for a long time. It doesn't do much good to have a "trusted" third party certifying a digital signature if that third party disappears, loses data, or is found out to have some serious security breach in its infrastructure.

In view of these problems, a system is needed that will translate the direct trust from signer to recipient that self-authenticating ink signatures now provide into the realm of digital signatures. The solution, it turns out, is combining technology with the

trusted authentication that ink signatures and signature witnesses have established over hundreds of years of history.

II. THE COVENANT - AN ANCIENT CONCEPT APPLIED TO TECHNOLOGY

The Covenant Trust Model relies on a person's self-certification of his or her public key and a covenant by that person not to repudiate the public key. The "Covenant of Non-repudiation" legally binds the owner of the public key to any digital signatures created with the corresponding private key. Thus, the liability for proper usage of the private key is placed on the shoulders of the person owning the public key, where it belongs, and legal reliance can be placed upon the public key and any electronic record signed with the corresponding private key.

The covenant is made in an Authentication and Certification Instrument (ACI), a legally signed paper document that contains an identification code positively identifying the public key in question. The document is signed in ink and witnessed by a notary public, thus invoking an authentication system whose trust has been established and is universally recognized by our legal system. An example ACI (see Appendix A-1) contains the following text:

> I acknowledge and understand that the consequence of executing this authorization and certification instrument ("Authorization") is that any electronic record accompanied by a digital signature that uniquely corresponds to both the document and the Public Key was signed by me, with a negligible level of doubt. I covenant with any bearer of this Authorization or facsimile copy thereof not to repudiate such digital signature unless I communicate (directly or indirectly) a revocation of the Public Key to the bearer in writing before the signature date.

The ACI includes security features, discussed below, that make it extremely difficult to forge with identification of a different public key, even in a facsimile copy. A person receiving a copy of the ACI (from the signer, from the Internet, wherever) is in possession of a legal instrument that authenticates a public key without the need for trusted third parties. The role of a third party, if one is used at all, is simply to distribute facsimile copies of the ACI. For additional security, the third party can apply its digital signature to the copies of the ACI it distributes to certify them as true copies of the original signed in ink. For example, the third party can authenticate PDF or TIFF files containing facsimile copies of ACIs with a standard SSL (Secure Sockets Layer) certificate issued by a conventional CA.

The conventional "hierarchical trust" model attempts to establish a chain of authenticity to supposedly trusted third parties who are presumed to be doing their jobs properly. In contrast, the covenant trust model establishes a chain of authenticity to a legal covenant, signed with a notarized ink signature on an ACI, in which a public key

owner promises not to repudiate digital signatures corresponding to that public key. The chain of authenticity can begin with initial reliance on the security features of a facsimile copy of the ACI and distribution of the ACI via a trusted web site, email sender, or remote-access viewing software. Higher up on the chain of authenticity, and still convenient to obtain, is digitally-signed certification of the copy by a trusted certifier. Still higher on the authenticity chain is the availability of ink-signed certified copies of the ACI by the original signer or, for a fee, by a trusted certifier. The ultimate link in the chain of authenticity can be provided by making the original notarized, ink-signed ACI paper available for inspection by experts, judges, juries, or attorneys during dispute resolution.

B. IMPLEMENTATION OF COVENANT TRUST VIA THE INTERNET

I. OVERVIEW

A new type of "Certification Authority" will be deployed at **SelfCertify.com** based on the covenant trust model. Selfcertify.com (discussed here in the present tense for convenience) is a certification authority only in the sense that it registers public keys and the identity of persons who claim to own those keys, and certifies that copies of ACIs it distributes are true copies of originals in its possession. It does not certify the identities of the person claiming to own the public keys - those persons make that certification themselves in the ACI.

In addition to registering public keys and distributing ACIs for authentication of those keys, SelfCertify.com can provide standardized digital certificates (e.g., using the X.509 standard) to ensure that its subscriber's public keys can be validated in a manner compatible with conventional public key infrastructure. Again, SelfCertify.com does not pretend that the trust imparted by its digital certificates is based on its confirmation of the identity of its subscribers. Instead, SelfCertify.com makes a policy of only issuing certificates for public keys that subscribers have self-certified with their notarized ink signatures in ACI documents. By signing a public key with its X.509 certificate, SelfCertify.com simply indicates that it has reviewed the original ink ACI and that a copy of the document can be freely downloaded from its Web server.

The use of X.509 or other standard certificates permits SelfCertify.com to live in the world of conventional CAs even though it is based on an entirely different trust model. Users who accept the covenant trust model can install SelfCertify.com's root CA certificate (the "grandfather" certificate that validates all of its individual certificates) into their Web browsers and e-mail applications. As the covenant trust model gains

acceptance in E-commerce, the manufacturers of Netscape Navigator and Internet Explorer can be expected to incorporate SelfCertify.com's root CA certificate into their browsers, alongside the certificates of VeriSign, entrust, and dozens of other CAs. Subscribers who use PGP (Pretty Good Privacy) and are looking for a way to validate their public keys outside PGP's "web of trust" model can submit their public keys to SelfCertify.com for it to be signed by SelfCertify.com's own PGP signature.

Because covenant trust does not require a trusted third party, subscribers' public keys can be validated directly from the subscriber's ACI. The public key of a SelfCertify.com subscriber can be validated by freely downloading a copy of the subscriber's ACI and checking its positive identification of the public key. Thus, no CA certificate is required at all. In fact, subscribers can directly distribute copies of their ACI to anyone who will be relying on signatures corresponding to their public keys.

II. EXAMPLE TRANSACTION USING SELFCERTIFY.COM

Below is a brief description of an example transaction based on covenant trust. In this example transaction, SelfCertify.com serves as a third party for the following:

1. Freely distributing a compact cryptographic software module to signer and recipient with instructions for secure use. The parties use the software for generation of the signer's private/public key pair, generation of the signer's digital signature on an electronic record, and validation of the digital signature against the signer's public key.
2. Accepting credit card payment (with SSL encryption), public key codes, and full legal names of new subscribers to SelfCertify.com.
3. Issuing blank ACIs to new subscribers, upon payment, with instructions for use.
4. Scanning original signed ACIs received from new subscribers and posting digitally certified copies on the web for free downloading.
5. Retaining original ACIs in a vault for inspection by experts, judges, juries, or attorneys during dispute resolution.

For convenience, this example refers to a widget vendor named Alice and a purchaser named Bob. (These names seem to be used in just about every published example of cryptographic transactions.) Alice wishes to sign a purchase agreement acknowledging Bob's payment of $1M for 10,000 widgets and promises to deliver the widgets immediately. Bob wants to make sure that Alice, the president of Widgets Inc., is the person signing the agreement and not some "man-in-the-middle" imposter.

- **Signer Enrollment**

Alice visits SelfCertify.com and quickly downloads a copy of "SelfCertify", a simple, compact, secure, and free cryptographic software application for Windows 98/NT/2000, with versions available for various other operating systems. The SelfCertify software installs to the Windows tray as an icon, with various functions selectable by right-clicking on the icon. If she wishes to avoid the need for installation, Alice has the option of simply downloading a single executable file to her desktop and running it from there. For maximum convenience (but possibly less security), a Java version of the software can be offered for execution in a web browser. Because SelfCertify.com serves its pages under SSL with a certificate issued by a conventional CA, Alice is assured that the software is authentic and trustworthy. For additional assurance, Alice reviews statements on the security of the software, written and digitally signed by various cryptographic experts, and validates the signatures of the statements before relying on the software.

Alice then follows the procedures outlined on SelfCertify.com for generating a public key from a secure passphrase. (See Appendix X.) She then gets out her credit card and subscribes to SelfCertify.com with her credit card number, public key code, and full legal name.

Selfcertify.com then issues Alice a custom-generated PDF file, from which Alice obtains two printed pages. The first page is a blank ACI with a space for her driver's license or other photographic ID and the second page is customized security paper with Alice's key code printed repeatedly in the background in an outline font.

Alice tapes her driver's license to the blank ACI in the space provided and places it on the glass of her photocopier, with the security paper at the top of her photocopier's paper supply. She then photocopies the blank ACI to produce an ACI, ready for her signature, with outline digits of her key code throughout its background.

Alice then checks the key code against her public key to make sure it is accurate, goes to the Notary Public down the hall, and executes the ACI in the presence of the notary. The notary examines Alice's driver's license, notes (in the ACI) any security features of it such as a hologram or colored background lines, and signs and stamps the ACI. Alice has now entered into a legally binding covenant with any person bearing the ACI or a facsimile copy of it. (So that she can keep a copy for her files and make certified copies herself, Alice elects to prepare and execute two original copies of the same ACI before the notary.)

Alice mails the executed ACI to SelfCertify.com. Within a few days, SelfCertify.com scans the ACI and posts a copy of it on its web site in PDF or TIFF format. Selfsertify.com stores the original ACI in a vault for possible inspection in the future by experts, judges, juries, or attorneys during dispute resolution. Selfcertify.com then emails Alice the following message:

> Your Authorization and Certification Instrument (ACI) has been recorded and you are now listed as a fully enrolled subscriber of **SelfCertify.com** with key ABC01. Once you enter the enrollment password "3f8u2b" in your SelfCertify software, your software will automatically download the latest copy of our public key registry (now including your key) and will automatically validate your digital signatures with the following text in any messages you sign: "The following text has been signed with a public key registered as key ABC01 at SelfCertify.com. Alice B. Costas has signed a written covenant not to repudiate digital signatures created with this public key. To view a copy of this document, click here. The code of this public key is BD7D F2FD EC1C DF14 4811 574F F7CE 7D1E 6EB6 F7E9 CCF7 208B." Persons relying on your digital signature will be able to easily download and inspect a copy of your ACI to legally bind you to that signature.

- **Signer's Digital Signature of Electronic Record**

In her email software, Alice selects the text of her purchase agreement with Bob and right-clicks on the SelfCertify icon in the Windows tray. She then selects the menu item "sign" and, when prompted, enters her private key passphrase. She will probably have to look the passphrase up from a piece of paper in her purse the first few times she uses it. Later, she will put the piece of paper in her safe or destroy it if she trusts her memory enough. If she forgets or loses the passphrase, it's not a big deal. She only needs to create another public key from a new passphrase, cancel her original ACI, and request another one to continue signing records.

As soon as Alice has entered her passphrase, the text she selected in her HTML-formatted email is replaced by text that is identical (including any formatting) except for a block of hexadecimal codes and the following statement in a reduced-size font:

> I, Alice B. Costas, have signed this document with my public key, which is registered as key ABC01 at **SelfCertify.com**. To verify this signature, click on http://SelfCertify.com/validate to download a compact, virus-free signature verification program that confirms the signature and public key. The software will allow you to obtain a copy of a paper document that you can use to legally bind me to this digital signature. You can also independently validate the public key by clicking on http://SelfCertify.com/?ABC001 to view a digitally certified copy of the document.

The formatting of the original text is preserved in the signed version. There is no header to the block of signed text because the SelfCertify software automatically calculates the beginning of the signed text block based on the number of signed characters, which is recorded in the signature block. Alice is free to select only a portion

of the text for signature. For example, she may choose not to include letterhead at the top of her letters in the block of text she signs.

Alice can also use S/MIME email software such as Netscape Messenger or Outlook Express to sign email messages using conventional, standardized digital signature technology and the Covenant Trust model, without the need for the SelfCertify.com software. However, she needs to sign an ACI with the SHA1 fingerprint of her S/MIME public key (called a "Digital ID") to authenticate it under the Covenant Trust model. SelfCertify.com then can issue a certificate for her S/MIME public key to authenticate it, based on her ACI.

- **Recipient's Validation of Digital Signature**

Bob receives Alice's digitally signed purchase agreement and downloads the SelfCertify software from the link provided in Alice's signature block. He also downloads a copy of her ACI. Once the software has been installed as an icon, Bob selects Alice's entire e-mail and right-clicks on the icon, then selects "Verify." A window pops up that says:

> The following text has been signed with a public key registered as key ABC01 at SelfCertify.com. Alice B. Costas has signed a written covenant not to repudiate digital signatures created with this public key. To view this paper, click **here**. The code of this public key is BD7D F2FD EC1C DF14 4811 574F F7CE 7D1E 6EB6 F7E9 CCF7 208B.

Since this is a $1M deal and he has never used the software before, Bob is not content with the software's assertion that Alice has entered into a legally binding covenant not to repudiate her digital signature with this key. Plus, Bob wants to have his lawyer look over the language of the covenant. So he clicks on the "here" link and a viewer window pops up with a TIFF copy of Alice's ACI. He prints out the ACI, notes that Alice's signature (which he recognizes from previous paper-based contracts) has been notarized and that the key code in the ACI is reproduced throughout the background of the document as vertically oriented digits in various outline fonts. The digits intermingle with the signatures, notary stamp, handwritten annotations, and images from Alice's driver's license. The key code digits even show up in the background of Alice's photograph in her driver's license.

Bob needs no further convincing that Alice was the one who signed purchase agreement. His lawyer, however, wants him to check out SelfCertify.com's SSL certificate for the copied ACI. Bob downloads the ACI copy from SelfCertify.com and, with the image of the ACI in his Web browser, clicks on the "security" button of the

browser. The browser provides a certificate issued to SelfCertify.com from a major CA, and Bob's lawyer is satisfied.

If Alice uses S/MIME to digitally signed her message, Bob can simply trust her S/MIME "Digital ID" based on the certificate SelfCertify has issued for it. Thus Alice and Bob can use the Direct Trust model with S/MIME signatures and conventional digital certificates, trusting selfcertify.com as a CA only for inspecting and verifying Alice's CA against the standard covenant language of the ACI, which is published at SelfCertify.com.

Alternatively, Bob can download and review Alice's ACI for her "Digital ID" from the web site of SelfCertify.com. If Bob chooses to download Alice's ACI, he will need to open Alice's "Digital ID," look for her SHA1 fingerprint, and compare it to the fingerprint printed on her ACI. This alternative procedure, while requiring an extra step, provides S/MIME signatures based more directly on the Covenant Trust model, moving closer to the ultimate link in the chain of authenticity, which is the original notarized, ink-signed ACI paper.

C. THE UNDERLYING TECHNOLOGY

The following is a brief listing of various aspects of the inventions discussed in this appendix:

- The key code in the ACI can be printed throughout the background of the entire paper as vertically oriented digits in various outline fonts. The font types, sizes, spacings, and line spacings are varied pseudorandomly in each ACI to make it difficult for an attacker to create an identical field of digits, which the attacker could use to remove the digits (by an XOR operation) from the ACI and substitute his or her own digits. Every bit of text and authenticating indicia in the ACI has background digits running through it. This feature (and possibly other features such as varying the spacing between digits of the text in a coded manner) protects both the signer of the ACI and the person relying on the ACI.
- The ACI can be created with a two-step procedure using a first page that is a blank ACI with a space for her driver's license or other photographic ID and a second page that is customized security paper with the subscriber's public key code printed repeatedly in the background in an outline font. The subscriber tapes his or her photo ID to the blank ACI in the space provided in places it on the glass of her photocopier, with the security paper at the top of the photocopier's paper supply. The blank ACI is then photocopied to produce an

ACI, ready for the subscriber's signature, with outline digits of her key codes throughout its background.

- The ACI can include language that makes it the only printed document of its type that can be accepted as valid. Additional ACIs can be signed electronically for additional keys, but they must be signed with the key that is certified in the original paper ACI. Selfcertify.com attaches digitally signed ACIs (for a fee) to the PDF or TIFF file in which it distributes the original paper ACI. By ensuring that the original printed document disclaims all other documents purporting to bear the singer's handwritten signature, a "strength in numbers" validity system is established that gives the authenticity of a widely distributed ACI, publicly available from a trusted server, far more weight than a single forged copy having a different key code. This feature helps to protect the signer of the ACI.
- The SelfCertify software can employ an ECDSA public key signature system with NIST Elliptic Curve P-192 (equivalent to 80-bit key length of symmetric cipher). The elliptic curve is described by a GF(p) field, where p is prime, to avoid recent attacks on elliptic curves from $GF(2^m)$, where m is a composite of smaller primes. See Smart, N. et al., "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," HP Technical Report HPL-2000-10, 17 January 2000.) A 192-bit public key can be represented by 12 groups of 4 hexadecimal digits. The short key length made possible by elliptic curve cryptography makes it easy for a recipient to visually verify the entire key code against the printed text of an ACI and the background security digits.
- The subscriber can be instructed to use a standardized, pronounceable passphrase made of "pseudowords" with alternating consonants and vowels. The passphrase is designed to be relatively easy to memorize, pronounce, and type and is very secure, with an entropy of about 2^{64}. The passphrase is created with simple, secure system using a piece of paper and a paper clip for random selection of digits.
- A SHA-1 hash of the passphrase can be used as the private key, with the subscriber's full legal name (from the SelfCertify.com directory) incorporated (transparently to the signer) into the passphrase as "salt." The use of salt prevents passphrase attacks using pre-computed hashes of passphrases within the standardized $\sim 2^{64}$ passphrase space.
- Formatting of signed text can be preserved after signing. The added text of the signature block is formatted in an unobtrusive font that does not detract from the appearance of the signed text. The text in the signature block includes a data field

with the number of characters being signed, which avoids the need for a distracting header block (e.g., "-----BEGIN PGP SIGNED MESSAGE-----" in PGP). Documents can also be signed as files, in which case the signature resides in a separate ".SIG" file, as is conventional.

- ACIs can be automatically opened from the software's signature validation window, based on the identification information in the signature block, and displayed or printed from a compact viewing window.

# # #

Alice wishes to become a subscriber to SelfCertify.com so that Bob will rely on her public key. However, she doesn't wish to go through the hassle of having a paper document sent to her and having it signed in the presence of a notary. She also wants people to be able to authenticate her public key by hearing a simple recorded statement by her. So, she chooses the "Verbal ACI" option on the SelfCertify.com Web site and enters her phone number and the fingerprint of her public key into the form. The Web site then lists a phone number and an access code and invites her to call the number.

She dials the number (making sure that call blocking is disables so that SelfCertify.com can detect the phone number she's calling from) and enters the access code using the touchtone keys of her telephone. She then enters into a brief oral exchange with a computer or human operator at SelfCertify.com. The exchange goes something like this:

SC: This telephone call is being recorded for the permanent records of SelfCertify.com, for the purpose of authenticating a public key you are certifying with SelfCertify.com. If you consent to this recording and proceeding with the certification process, please state "I agree" and then recite your full legal name and mailing address.

Alice: I agree. My name is Alice P. Costas, and my address is 537 Main Street, Anytown Arizona 12345.

SC: Now that we have your agreement to record this telephone call and proceed, we will ask that you carefully read the terms of the "Authentication and Certification Instrument." You will be asked to agree to the terms of that document, and your recorded verbal agreement will legally bind you to those terms as if you had signed the document with your ink signature. Please state "Yes, it is" to confirm with the statement entitled "Authentication and Certification Instrument" is now displayed on your web browser at **https://www.selfcertify.com/aci32776** and that the document refers to a public key with fingerprint 2355 7782 1193 8001. You will be given an opportunity to read the document in a minute if you haven't already done so. Right now, we just ask you to confirm that the document is being displayed.

Alice: Yes, it is.

SC: Now we will ask you to ensure that you have read the document. We recommend that you print the document for your records, as you will be bound to its terms if you proceed. Please say "I have read the document" when you have done so.

Alice: Yes, I've read the document.

SC: Now please confirm your legally binding agreement with the terms of the document entitled "Authentication and Certification Instrument, " displayed on your web browser at **https://www.selfcertify.com/aci32776** and referring to a public key with fingerprint 2355 7782 1193 8001, on this___ day of _____,___ by stating "Yes, I agree to the terms of the document."

Alice: Yes, I agree.

SC: Sorry, you need to state exactly, "Yes, I agree to the terms of the document."

Alice: Yes, I agree to the terms of the document.

SC: Thank you. This includes your verbal certification of your public key. Thank you.

<End of Recording>

SIGNED MEDIA STREAMS

This invention is another aspect of the general concept of calculating a digital signature based on all of the contents of an electronic record except an excluded signature portion. (The general concept advantageously gets around the circular problem of a document essentially signing itself.)

With modern technology, it is difficult to place trust in the authenticity of a video or audio recording. Portions of the recording can be digitally modified in a way that even a careful observer cannot detect. One advantageous aspect of this invention permits a video or audio recording to be validated without requiring special a recording format. Another advantageous aspect of this invention performs frame-by frame authentication of a recording to ensure that the observer is alerted to unauthenticated portions of the recording.

An attached page includes two figures, one depicting the spectrum of an audio recording with an out-of-band transmission of digital signature information, and the other depicting the frame-by frame computation and transmission of digital signatures. During frame T2, a digital signature S1 is computed based on digital samples of the recording within frame T1, and the signature S1 is transmitted (along with other digital samples of the recording) in frame T3. During frame T3, a digital signature S2 is computed based on digital samples of the recording within frame T2, and the signature S2 is transmitted (along with other digital samples of the recording) in frame T4 (not shown). Optionally, digital signature S2 can include (or consist of) an aggregate signature formed from a bitwise modulo sum of the signature and the previous signature.

Advantageously, the video or audio recording can be transmitted and stored independent of any specific digital format, as long as the modulated digital signature information is faithfully conveyed along with the recording information. To allow for degradation of the recording, the signature is preferably computed based on truncated samples. An example of a truncated sample is an audio sample (e.g., noisy 16 bits) that is set to the nearest value within a truncated binary set (e.g., 8 bits). The likelihood of a noisy value being pushed over a boundary between value within the truncated set is small, about 2^(x-y) where x is the full set size in bits and y is the truncated set size in bits.

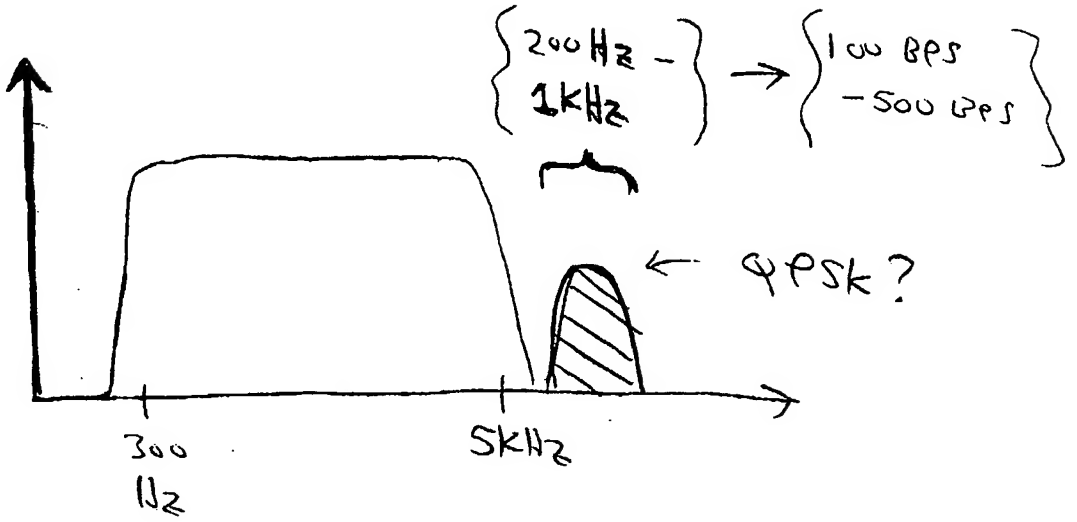
With x-y=8, the likelihood is 1 in 255, which represents a fairly significant probability of signature error in a given frame. Consequently, the number of samples in a frame should be kept fairly small.

More preferably, speech statistics (i.e., "feature vectors") used in speech recognition (13 spectral magnitude values within 10 ms frames) can be derived from the

recording. If the derivation of the statistics can be made robust in the presence of noise, less signature errors will result.

The media player can authenticate the media stream by including a visually intuitive authentication display. The display can take into account a running statistic of frame authentications, for example by slightly decreasing a "gas gauge" bar for each signature error in a moving average of 32 frames. If frames are short enough, the speech content will not be suspect unless a large gap occurs.

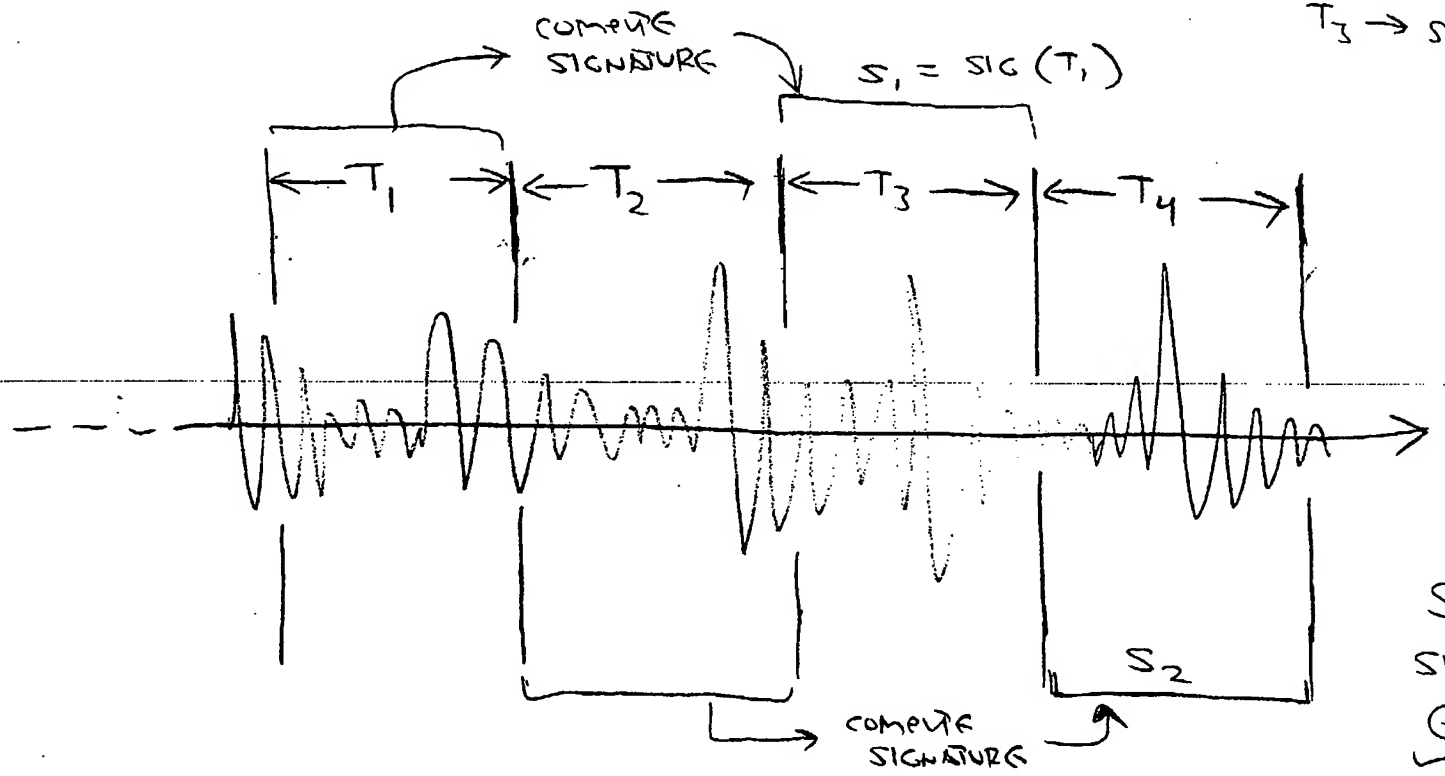
# # #



$T_1 \rightarrow SIG \rightarrow S_1$, TX IN T_3

$T_2 \rightarrow SIG \rightarrow S_2$, transmit IN T_4

$T_3 \rightarrow SIG \rightarrow S_3$, IN T_5



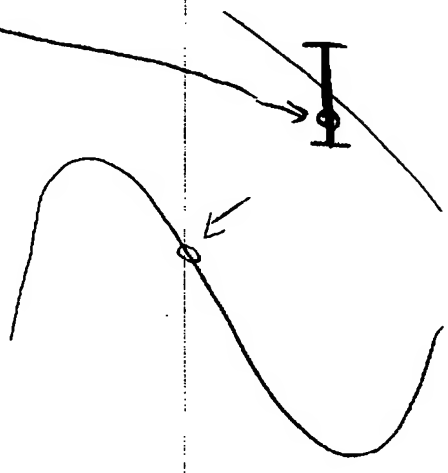
$S_2 =$ SIG (T_2) $\oplus$ S_1

optional

* SIGNATURE should be compact (ECC)

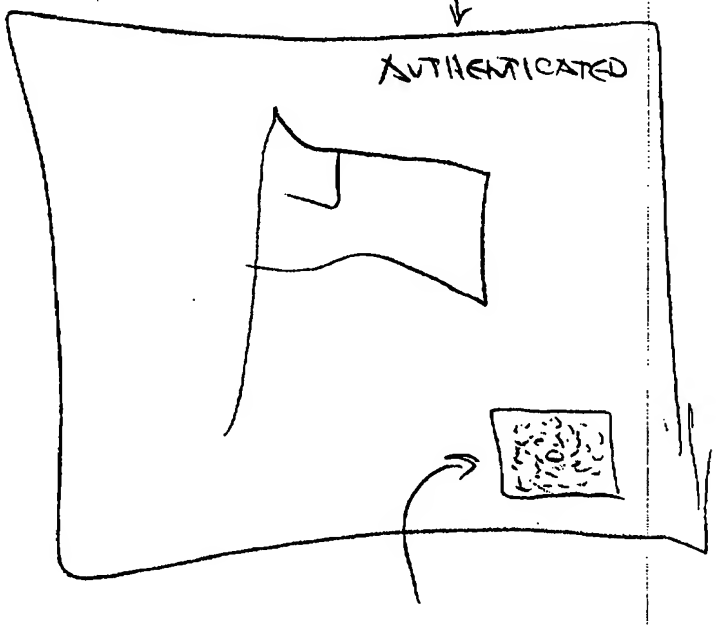
* Can calculate signature based on truncated sample words

should be set to nearest value* in truncated word length to allow for some noise.



* 256-bit signature (just a guess)
10-second ~~blocks~~ frames
= 25 bps ← can be subaudible or DSSS

* Can put signature barcode (2D) in video image. Will be blanked out in calculation of that ~~block's~~ signature frame



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.